Security in Electronic World

Jujhar Singh

Assistant Professor, Department of Computer Science & Applications
Guru Nanak Khalsa College
Karnal (Haryana)
India

ABSTRACT

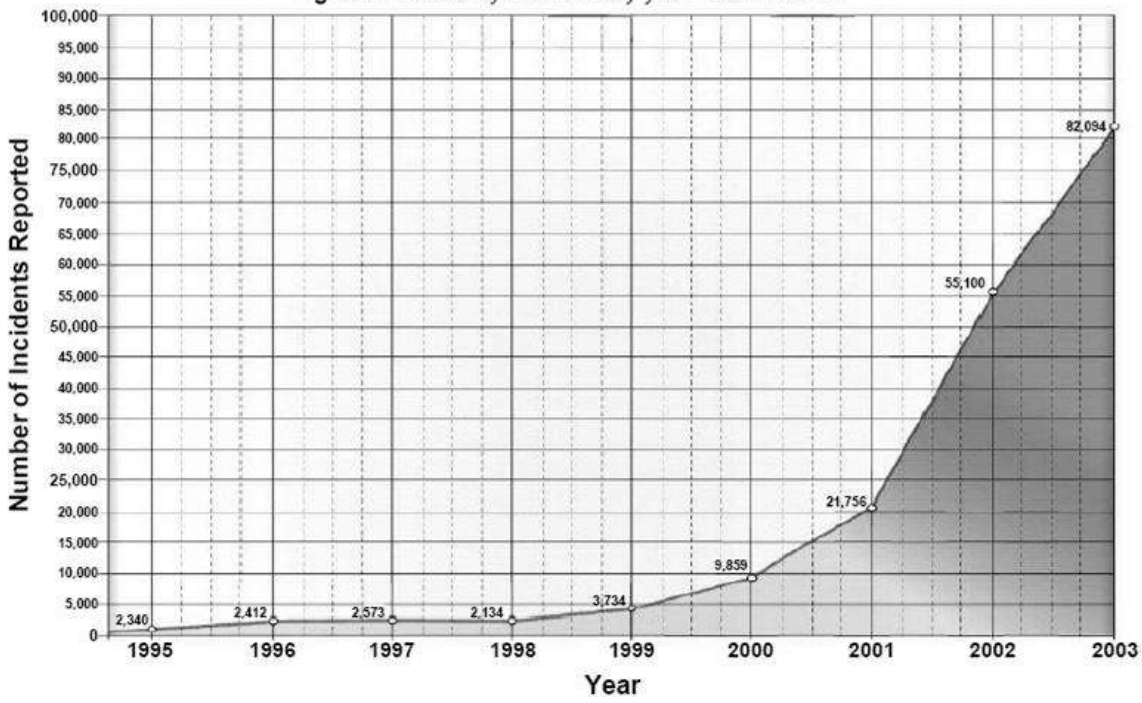
In last two decade there is growth of data communications networks development in electronic commerce. Qualification as an SSCD (Secure Signature-Creation Device) is necessary for a digital signature (standard electronic signature) solution to comply with the EU Directive for Electronic Signatures. An SSCD is defined by the EC Directive 99/93 on Electronic Signatures as follows: Secure signature-creation devices must, by appropriate technical and procedural means, ensure: The signature-creation data used for signature generation can occur only once, and that their secrecy is reasonably assured. The signature-creation data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology. The signature-creation data used for signature generation can be reliably protected by the legitimate signatory against the use of others. Secure signature-creation devices must not alter data to be signed or prevent such data from being presented to the signatory prior to the signature process.

INDEX TERMS: Symmetric Key, Public Key, Digital Signature, Electronic Signature, Digital Certificate

I. INTRODUCTION

Electronic World is a new and fast moving Technology and as such, is still being defined and most probably will always be "still defined". Security incidents are rising at an alarming rate every year [Figure-1]

Figure 1 – Security incidents by year – CERT.ORG



Electronic commerce, as exemplified by the popularity of the Internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce. Even though SSL is extremely effective and widely accepted as the online payment standard, it requires the customer and merchant to trust

each other: an undesirable requirement even in face-to-face transactions, and across the Internet it admits unacceptable risks. Visa and MasterCard and a consortium of 11 technology companies made a promise to banks, merchants, and consumers:[6] they would make the Internet safe for credit card transactions and send electronic commerce revenues skyward. With great fanfare, they introduced the Secure Electronic Transaction protocol for processing online credit card purchases. In Electronic Record, We can easily make copies, Is Very fast distribution, Easy archiving and retrieval, Copies are as good as original, Easily modifiable, Environmental Friendly. Here are a few examples of things that have been, can or will be done online:

Banking, bill payment, home shopping, stock trading, auctions, taxation, gambling, micro payment (e.g., pay-per-downloading), electronic identity, online access to medical records, virtual private networking, secure data archival and retrieval, certified delivery of documents, fair exchange of sensitive documents, fair signing of contracts, time-stamping, notarization, voting, advertising, licensing, ticket booking, interactive games, digital libraries, digital rights management, pirate tracing, …[2]

II. FOCUS ON SECURITY

Main key points of security

Privacy/Confidentiality: preventing disclosure of information to unauthorized individuals or systems
Authenticity: Ensuring that the user, data, transactions, communications or documents are genuine
Integrity: Data cannot be modified without authorization
Non-Reputability: One party of a transaction can not deny having sent/received a transaction

The internet Security program emphasizes to secure Electronic data. Modern secure protocols are based on a number of underlying cryptographic techniques. In this section we explain the commonly used techniques.

We discuss five subject areas:[8]

a. Symmetric key (or bulk) encryption

b. Public key(Asymmetric key) encryption

c. Secure hash (or digest) functions

d. Digital Signatures

e. Electronic Signature

a) SYMMETRIC KEY ENCRYPTION [7]

This is a grown-up version of the kind of secret code that most of us played with at some time during childhood. Usually these use a simple character replacement algorithm; if you want to encrypt a message, you just replace each letter of the alphabet with another. For example:

Original letter: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Replacement: GHIJKLMNOPQRSTUVWXYZABCDEF

In this case the letters in the alphabet have just been shifted seven places to the right, so HELLO WORLD would translate to NKRRU CUXRJ. The premise on which this code is based is that both the sender and the receiver know a common key, in this case the number of places to shift the letters. This shared secret allows the receiver of the message to reverse the encryption process and read the scrambled message as shown in figure 2. Symmetric encryption algorithms used by computers have the same elements as this simple example, namely a mechanism to scramble the message (also known as a cipher) and a shared secret (a key) that allows the receiver to unscramble the encrypted message.

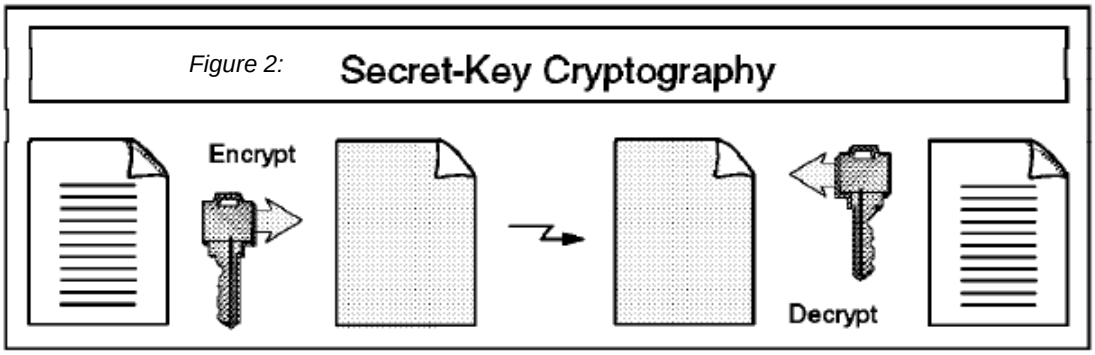


Figure 2:

The strength of a symmetric key cipher of this kind is dictated by a number of factors. For example, It is important that it effectively randomizes the input, so that two related clear-text messages do not produce similar encrypted results.

COMMON SYMMETRIC KEY ALGORITHMS

DES[6]**:** The **Data Encryption Standard** (**DES**) is a block cipher that uses shared secret encryption. It was selected by the National Bureau of Standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on a symmetric-key algorithm that uses a 56-bit key. The algorithm was initially controversial with classified design elements, a relatively short key length, and suspicions about a National Security Agency (NSA) backdoor. DES consequently came under intense academic scrutiny which motivated the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; in January, 1999,distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes

RC2/RC4[6] **:** These related ciphers were developed by RSA Data Security, RC2 is a block cipher similar to DES, whereas RC4 operates on a stream of data. They both use a 128-bit key, but they support key masking. This means that part of the key may be set to a known value so that the effective key size is whatever remains from the 128-bit total.

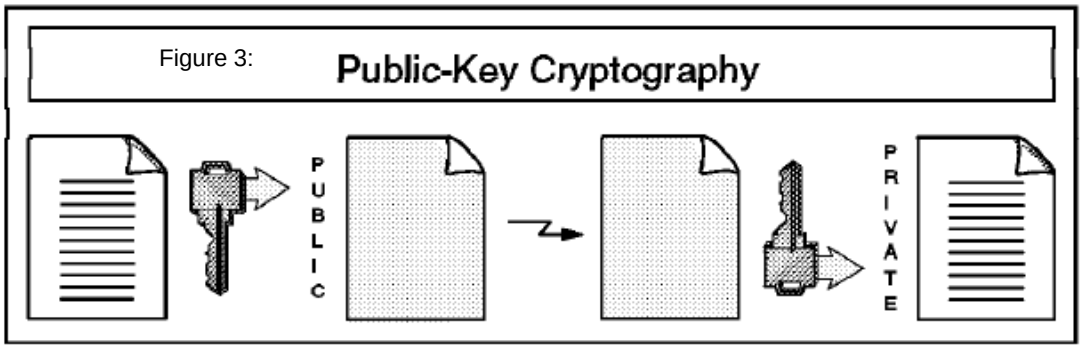
IDEA[6] : The International Data Encryption Algorithm is another block cipher, in the mold of DES. It uses a 64-bit block size and a 128-bit key. IDEA is the bulk encryption algorithm used by Pretty Good Privacy (PGP).

b) PUBLIC KEY (ASYMMETRIC KEY) ENCRYPTION[1]

A non-mathematician can intuitively understand how a symmetric key cipher works by extrapolating from a familiar base. However, public key mechanisms are much less accessible to the lay person. In fact, it sometimes seems more like magic than technology. The fundamentals of public key encryption are:

1. Instead of a single encryption key, there are two related keys, a key pair .
2. Anything encrypted using one of the two keys can only be decrypted with the other key of the pair.

Figure 3:



Let us say that two people, Ram and Sham, want to exchange messages using a public key algorithm. Sham generates a key pair and places one of the keys, the private key in a safe place. He sends the other half of the key pair (called, naturally, the public key) to Ram. Ram can now encrypt a message using the public key and only the owner of the matching private key, Sham, can decrypt it by the private key. Of course, if Sham wants to send a reply, Ram needs to create his own key pair and send the public key to Sham.

COMMON PUBLIC KEY ALGORITHMS

RSA[1]: The key in this case is actually a very large number. Very approximately, an RSA key size of 1024 bits corresponds to a full-strength Symmetric key of 64 bits or more.

SECURE HASH FUNCTIONS[1]: The third tool in our encryption armory is not actually an encryption mechanism at all. A secure hash is a way of creating a kind of "fingerprint" of a message. A secure hash function has three main attributes:

1. It takes a message of any size and generates a small, fixed size, block of data from it (called a message digest). Re-executing the hash function on the same source data will always yield the same resulting digest.
2. It is not predictable in operation. That is to say, a small change in the source message will have an unpredictably large effect on the final digest.
3. It is, for all intents and purposes, irreversible. In other words there is no way to derive the source data, given its digested form.

c) DIGITAL SIGNATURE[13]

For digital signatures there is a key pair: a secret ***digital signature key***, which is used for signing data items, and a public ***digital signature verification key***, which is used by others to check if a signature was made with the related signature key. Although the term 'signature' is used for both, in practice digital signatures and handwritten signatures have quite different characteristics. If a digitally signed document is tampered with in any way, its digital signature will not verify. However, the private key that generated the signature can be used by anyone who can gain access to its value, making it more like a seal. On the other hand, a written signature is linked in a biometric way to its owner but its use on a document does not prevent the latter's subsequent, Undetected modification.

A written signature is evidence that the person acted on a document whereas a digital signature is evidence that a given private key acted on a document. Usefully, a digital signature also tells us that the document has not been changed since the signature was made (the way

digital signatures work provides this confidence). However, without further information, a digital signature provides no evidence about the participation of any particular person. If the secret signing key is kept under the control of a single person, then one can assume that the key acts as an agent for that person and one might assume that documents signed by the key were actually signed by the person. This is analogous to a check-writing machine. As long as the machine is kept well guarded and access to the machine is only by authorized signers, the machine signature can stand for the human signature it replaces. However, establishing that a signing key was under the control of a particular person at the time of a particular signature and that the person actually knew what he was signing with that key is a very complicated process.

d) ELECTRONIC SIGNATURE[13]

An electronic signature is defined as an electronic sound (e.g., audio files of a person's voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record. An electronic signature is easy to implement, since something as simple as a typed name can serve as one. Consequently, e-signatures are very problematic with regards to maintaining integrity and security, as there is nothing to prevent one individual from typing another individual's name. Due to this reality, an electronic signature that does not incorporate additional measures of security (similar to a digital signature, described above) is considered an insecure way of signing documentation.

DIFFERENCE BETWEEN ELECTRONIC & DIGITAL SIGNATURE

A digital signature often referred to as advanced or standard electronic signature is a sub group within electronic signatures which provide the highest form of signature and content integrity as well as universal acceptance. The digital signature is based on Public Key Infrastructure (PKI) and is a result of a cryptographic operation that guarantees signer authenticity, data integrity and non-repudiation of signed documents. The digital signature cannot be copied, tampered or altered. In addition, because they are based on standard PKI technology, digital signatures made within one application (e.g. Microsoft® Word, Adobe® PDF) can be validated by others using the same applications. On the other hand, an electronic signature is a proprietary format (there is no standard for electronic signatures) that is an electronic data, such as a digitized image of a handwritten signature, a symbol, voiceprint, etc., which identifies the author(s) of an electronic message. An electronic signature is vulnerable to copying and tampering, making forgery easy. In many cases, they are not legally binding and will require proprietary software to validate the e-signature.

CONCLUSION:

The security issues in our Electronic systems as described in this paper identify some of the work that needs to be done, and the urgency with which concerns need to be addressed. Dependence on some of the IT-based infrastructures in several countries is such that serious national consequences could result from the exploitation of their vulnerabilities. The Indian IT Act 2000 specifies that authentication must be by Digital Signatures based upon Asymmetric Key Cryptography and Hash Functions. The National Root CA uses a 2048 bit RSA key pair. Other CA and end entities use 1024 bit RSA key pairs. The IT act provides the Controller for Certificate Authorities (CCA) to license and regulate the working of CA.

In India there are National Root CA which issues CA certificates for licensed CA's and 7 CA's licensed under the National Root CA are: Safe Scrypt, TCS, MTNL, nCode, National Informatics Center, IDRBT, 3i InfoTech.

REFERENCES:

[1] Loren M. Kohnfelder, "Towards a Practical Public-key Cryptosystem", May 1978, p.15.

[2] Ross Anderson et al, "The Global Trust Register", Northgate Consultants Ltd, 10 Water End, Wrestlingsworth, Sandy, Bedfordshire Sg19 2HA, United Kingdom.

[3] Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, John F. Farrell, "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments", National Security Agency.

[4] Carl M. Ellison, "Infrastructure Needs For Electronic Commerce and Personal Use", CyberCash Inc.

[5] Matt Blaze, Jane Feigenbaum and Jack Lacy, "Decentralised Trust Management", AT&T Research.

[6] DES http://en.wikipedia.org/wiki/Data_Encryption_Standard
RC2/RC4 http://en.wikipedia.org/w/index.php?title=Special%3ASearch&search=RC2%2FRC4
IDEA http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm

[7] Secure Electronic Transactions: An Overview http://www.davidreilly.com/topics/electronic_commerce/essays/secure_electronic _transactions.html

[8] Evaluation of Security Level of Cryptography: RSA-OAEP, RSA-PSS, RSA Signature http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1049_ace.pdf

[9] Brush, C., Surcharge for Insecurity. Information Security Magazine, July 2001: http://www.infosecuritymag.com/articles/july01/departments_news.shtml CERT/CC, CERT/CC Statistics 1988-2002, 5 April 2002: http://www.cert.org/stats/cert_stats.html

[10] Windows 2003 PKI Operations Guide: http://technet2.microsoft.com/WindowsServer/en/Library/e1d5a892-10e1-417c-be13-99d7147989a91033.mspx?mfr=true

[11] Configuring 802.1x wireless encryption: http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

[12] Setting up a certificate of authority: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/xmlsdk/html/29ff74a2-249a-4ecf-8a2a-ff0ba572e4db.asp

[13] Digital Signature http://www.arx.com/digital-signatures-faq